

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner,

v.

INTELLECTUAL VENTURES, II LLC,
Patent Owner.

IPR2024-00124
Patent 7,325,140 B2

Before HYUN J. JUNG, JOHN D. HAMANN, and STEPHEN E. BELISLE,
Administrative Patent Judges.

HAMANN, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Lenovo (United States) Inc. (“Petitioner”) filed a petition for *inter partes* review of claims 1–4, 6, 7, 10–14, and 16 (“the challenged claims”) of U.S. Patent No. 7,325,140 B2 (Ex. 1002, “the ’140 patent”). Paper 1 (“Pet.”). Intellectual Ventures II LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Institution of an *inter partes* review is authorized by statute when “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.108 (2024). Upon consideration of the papers, we conclude that the information presented shows that there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of at least one challenged claim of the ’140 patent.

A. *Real Parties-in-Interest*

Petitioner identifies itself and Lenovo Group Ltd. as real parties-in-interest. Pet. 82. Patent Owner identifies itself as a real party-in-interest. Paper 4, 2.

B. *Related Matters*

The parties identify *Intellectual Ventures II LLC v. Lenovo Group Ltd.*, 6:23-cv-00307-ADA-DTG (W.D. Tex.) as a matter that may affect, or be affected by, a decision in this proceeding. Pet. 83; Paper 4, 2.

C. *The Challenged Patent*

The ’140 patent “relates in general to . . . managing devices or systems in a communication network and more particularly to methods and apparatus for remote management of these devices or systems in a secure manner.” Ex. 1002, 1:19–23. The ’140 patent explains that “[i]n distributed

computer networks[,] the vast majority of the networking elements are not in the same geographic location or easily accessible by the skilled technicians or network administrators typically responsible for normal maintenance of the elements.” *Id.* at 1:27–31. Thus, “[i]n general, it is not practical to require physical access to the systems for general maintenance or troubleshooting and repair.” *Id.* at 1:39–41. “The costs would be prohibitive, both in time and person[ne], to require a skilled technician to be dispatched for every required activity on a system.” *Id.* at 1:41–43. “This has driven a strong requirement to provide for remote management of network elements and servers,” according to the ’140 patent. *Id.* at 1:43–45. However, “the security of the network elements and servers is a concern when remote management is allowed.” *Id.* at 1:56–57.

“It is important . . . to realize that opening up a device to remote management allows a larger window for attackers to utilize in an attack,” and thus, “[t]he use and security of remote management must be carefully considered.” *Id.* at 1:64–67. The ’140 patent explains that for known ways “to address most of the concerns” of remote management, “[i]t would take a number of different devices configured to work together,” which “would require a number of additional devices in an environment where rack space is very expensive.” *Id.* at 4:1–4.

In response, the ’140 patent “provide[s] for the secure management of devices without requiring additional devices taking up additional rack space by embedding the necessary hardware and software for secure management of the device in the device to be managed.” *Id.* at 4:7–11. More specifically, the ’140 patent describes “a Secure Management Access Control for Computer Chipset (SMACC) for inclusion in devices that are to

be enabled for remote management.” *Id.* at 5:48–52. Figure 1 of the ’140 patent is shown below.

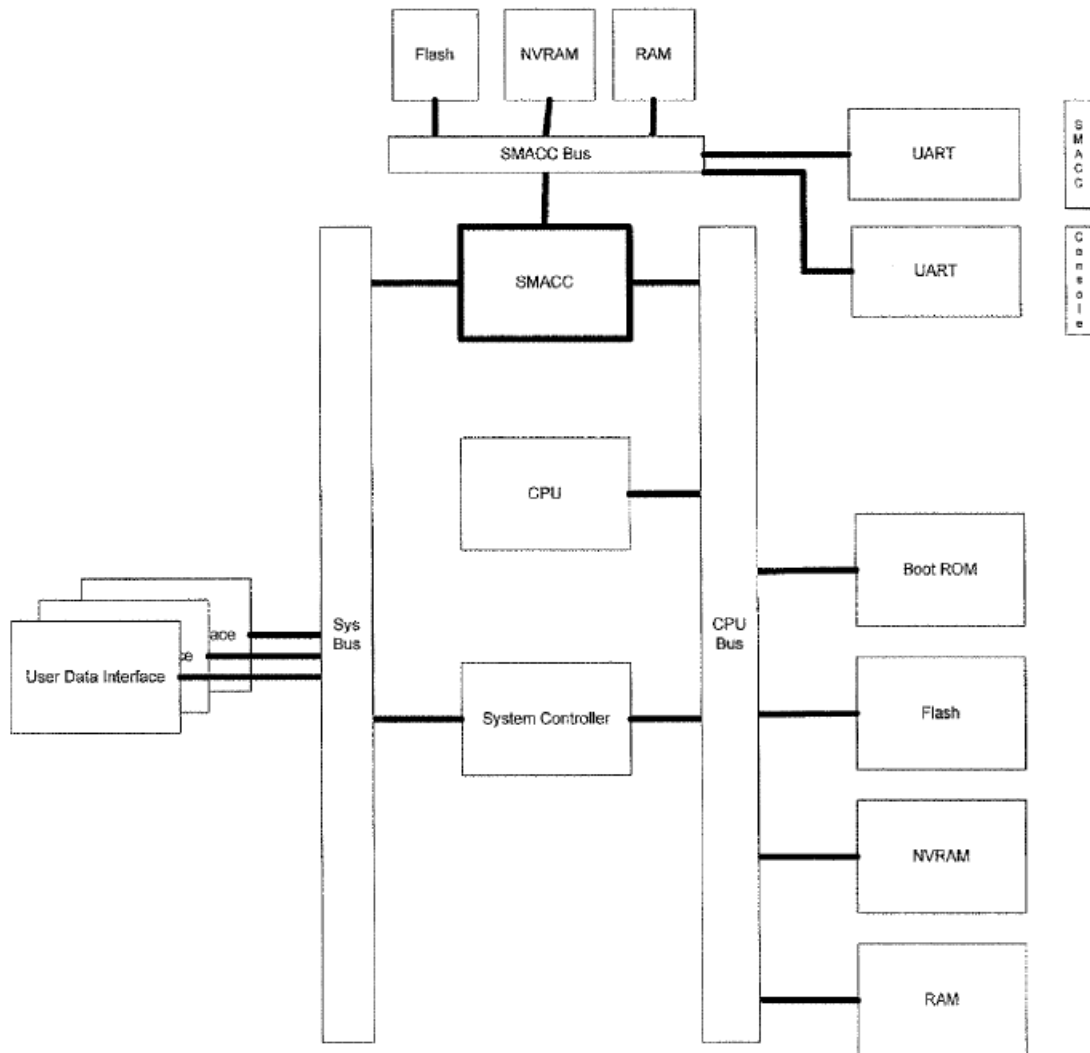


Fig. 1

Figure 1 “is a block diagram for an exemplary embodiment of the embedded SMACC” chipset and “illustrates the positioning of the SMACC chipset within the managed device.” *Id.* at 9:41–43, 10:64–65. As illustrated, “the SMACC processor has its own flash, Non-Volatile Random Access Memory (NVRAM), and Random Access Memory (RAM) for operating.” *Id.* at 10:66–11:1, Fig. 1. The SMACC is coupled both to the Central Processing

Unit (“CPU”) Bus and the System Bus of the managed device. *Id.* at Fig. 1. The System Bus also is coupled to User Data Interfaces for user data traffic. *Id.*

In addition, the ’140 patent discloses that “[r]emote management . . . can be provided in-band ([i.e.,]the remote administrator communicates with the system using the same network as the user data for the managed system).” *Id.* at 1:47–50. Moreover, the managed device can be configured with a Virtual Management Interface (“VMI”), which uses a Virtual Private Network (“VPN”) and “logically separates management traffic from user data traffic when a user interface on the managed device is going to be utilized for the network connection.” *Id.* at 11:60–67, 12:6–9.

D. The Challenged Claims

Petitioner challenges claims 1–4, 6, 7, 10–14, and 16 in this proceeding. Claim 1 is the sole independent claim. Claim 1 is illustrative of the challenged claims and is reproduced below:

1. A remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices, the remote device management system comprising:

at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data;

an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device; and

at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller,

wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.

Ex. 1002, 22:32–57.

E. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the '140 patent are unpatentable based on the following grounds:

Claim(s) Challenged	35 U.S.C. §¹	Reference(s)/Basis
1–4, 6, 7, 10, 11, 13, 16	103(a)	Neufeld ²
11, 12	103(a)	Neufeld, Syvanne ³
13, 14	103(a)	Neufeld, Fowler ⁴
1–3, 6, 7, 10, 11	103(a)	IPMI, ⁵ Lawrence ⁶
4	103(a)	IPMI, Lawrence, Leedy ⁷
11, 12	103(a)	IPMI, Lawrence, Syvanne
13, 14	103(a)	IPMI, Lawrence, Fowler
16	103(a)	IPMI, Lawrence, RFC1492 ⁸

¹ The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the '140 patent issued from an application having a filing date before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.

² US 2003/0226015 A1, published Dec. 4, 2003 (Ex. 1005, “Neufeld”).

³ US 2003/0097590 A1, published May 22, 2003 (Ex. 1016, “Syvanne”).

⁴ WO 01/31849 A1, published May 3, 2001 (Ex. 1040, “Fowler”).

⁵ IPMI – Intelligent Platform Management Interface Specification V1.5 (Rev. 1.1 dated Feb. 20, 2002) (Ex. 1020, “IPMI”).

⁶ US 7,269,639, issued Sept. 11, 2007 (Ex. 1043, “Lawrence”).

⁷ WO 2004/015764 A2, published Feb. 19, 2004 (Ex. 1045, “Leedy”).

⁸ RFC1492: An Access Control Protocol, Sometimes Called TACACS (July 1993) (Ex. 1013, “RFC1492”).

Pet. 1–2, 21–81. Petitioner submits in support of its arguments the Declaration of Sigurd Meldal, Dr. Scient. (Ex. 1003), the Declaration of Sigurd Meldal, Dr. Scient. (Ex. 1046), and the Declaration of Nathaniel E. Frank-White (Ex. 1039). Patent Owner submits in support of its arguments the Declaration of Dr. Steven Goldberg (Ex. 2001).

II. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962–63 (Fed. Cir. 1986)). “[O]ne or more factors may predominate.” *Id.*

Petitioner argues that one of ordinary skill in the art “would have had a Bachelors’ degree in electrical or computer engineering or a comparable field of study, plus approximately two to three years of professional experience in the field of computer and/or network design and security or other relevant industry experience,” and that “[a]dditional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education.” Pet. 7–8 (citing Ex. 1046 ¶ 54). Patent Owner does not address Petitioner’s definition, nor provide its own. *See generally* Prelim. Resp.

For purposes of this Decision, we adopt Petitioner’s definition of the level of skill for one of ordinary skill in the art. Pet. 7–8. We view this

definition for the level of ordinary skill as consistent with the '140 patent and the asserted prior art, and we apply it in our analysis below.

III. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we apply the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b), following the standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b); 83 Fed. Reg. 51,340, 51,340–41, 51,343 (Oct. 11, 2018). In applying such standard, claim terms generally are given their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner argues that the “said managed network element,” as recited in claim 1 means “said managed network device.” Pet. 9. At this stage, Patent Owner does not dispute this construction. We adopt Petitioner’s proposed construction for this term as it appears to be consistent with the Specification’s use of “element” as referring to networked devices, and with the overall claim. *See generally* Ex. 1002.

In addition, Petitioner argues that certain terms⁹ of claim 1 are means-plus-function terms, and as such, Petitioner identifies the recited function and its corresponding structure in the Specification. First, Petitioner argues that “an out of band access connection means” is a means-plus-function term with the recited function being “connecting said one or more network services or remote users with said secure management access controller for management of said network device.” *Id.* at 10. Petitioner argues that the function’s corresponding structure is “one or more of the following networks: a Public Switched Telephone Network (PSTN) (2:45–57, 3:2–4, 12:37–61), an Integrated Services Digital Network (ISDN) (2:45–57), a cellular network (6:14–21, 7:60–62, 12:37–61), an Ethernet network (12:37–61), a wireless network, and/or a Digital Subscriber Line (DSL) (12:37–61, 15:55–60), where the one or more networks use one or more of the following protocols: [Simple Network Management Protocol (“SNMP”)], TFTP, FTP, DNS, SysLog, Telnet, SSH, HTTP, HTTPs, point to point IP, and/or XML (8:30–38).” *Id.*

Second, Petitioner argues that “virtual management interface connection means” is a means-plus-function term with the following recited functions: “‘connecting said one or more network services or remote users with said secure management access controller’; (ii) ‘provides logical separation of management data from user data,’ and (iii) ‘utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access

⁹ Petitioner also identifies means-plus-function terms for claims 11, 13, 14, and 16. Pet. 11–13. We do not address those terms in this institution decision because our analysis below does not reach these claims, which are not separately argued by Patent Owner at this stage.

controller.”” *Id.* at 10–11. Petitioner argues that the functions’ corresponding structure is a VPN (6:22–44, 6:63–7:5, 12:5–21). *Id.* at 11.

Petitioner does not explain why we should adopt its proposed constructions for these means-plus-function terms. Rather, Petitioner states that it adopts the district court’s constructions for these terms from a related district court litigation. *Id.* at 9. We note, however, the following guidance for proceedings before the Board as it relates to claim construction:

The Board will determine the claim construction based on the record of the proceeding at issue. Thus, as in a district court proceeding, the parties should point out the specific portions of the specification, prosecution history, and relevant extrinsic evidence they want considered, and explain the relevancy of any such evidence to the arguments they advance. Each party bears the burden of providing sufficient support for any construction advanced by that party.

Consolidated Trial Practice Guide (Nov. 2019)¹⁰ (“CTPG”) 46.

Patent Owner does not set forth any term for construction, nor address Petitioner’s construction arguments. *See generally* Prelim. Resp.

At this stage, we adopt Petitioner’s proposed constructions for these means-plus-function terms. Petitioner sufficiently identifies the recited functions and the specific portions of the specification corresponding to each recited function. *See* 37 C.F.R. § 42.104(b)(3). And these proposed constructions are undisputed, at this stage. In addition, we consider the Construction Order from the related district court litigation, but we note that it provides no reasoning for why the terms were construed as they were. 37 C.F.R. § 42.100(b); Ex. 1042 (Claim Construction Order), 1 (“This order memorializes the Court’s final constructions of the disputed terms in this

¹⁰ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

case. The Court will issue memorandum opinion on these rulings in due course.”).

IV. PRINCIPLES OF LAW

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.¹¹ *See Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

V. ALLEGED OBVIOUSNESS OVER NEUFELD

Petitioner argues that Neufeld renders claims 1–4, 6, 7, 10, 11, 13, and 16 obvious. Pet. 21–43. For the reasons that follow, we determine that Petitioner establishes a reasonable likelihood that it would prevail in showing that this combination renders at least one of these claims obvious.

A. *Summary of Neufeld*

Neufeld “relates generally to computer security systems and, more particularly, to a technique for providing user profiles.” Ex. 1005 ¶ 2. In

¹¹ Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness at this stage. *See generally* Prelim. Resp.

particular, Neufeld teaches “[a] security system [which] includes different authentication levels and/or different privileges based on certain criteria.” *Id.* at code (57). “For example, if a user’s identity can be somewhat assured due to the directness of the connection, authentication may be less rigorous than in a situation where the connection is more remote, thus making the user’s identity less assured.” *Id.* Neufeld also teaches that “a user’s privileges may be restricted if the user accesses the system from a remote location or during non-business hours.” *Id.*

B. Challenged Claim 1

1. Remote Device Management Communication System

Petitioner argues that Neufeld teaches “[a] remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices, the remote device management system,” as recited in the preamble of claim 1. Pet. 21–25.

In particular, Petitioner argues that Neufeld’s Figure 1, shown below, supports that Neufeld teaches this limitation.

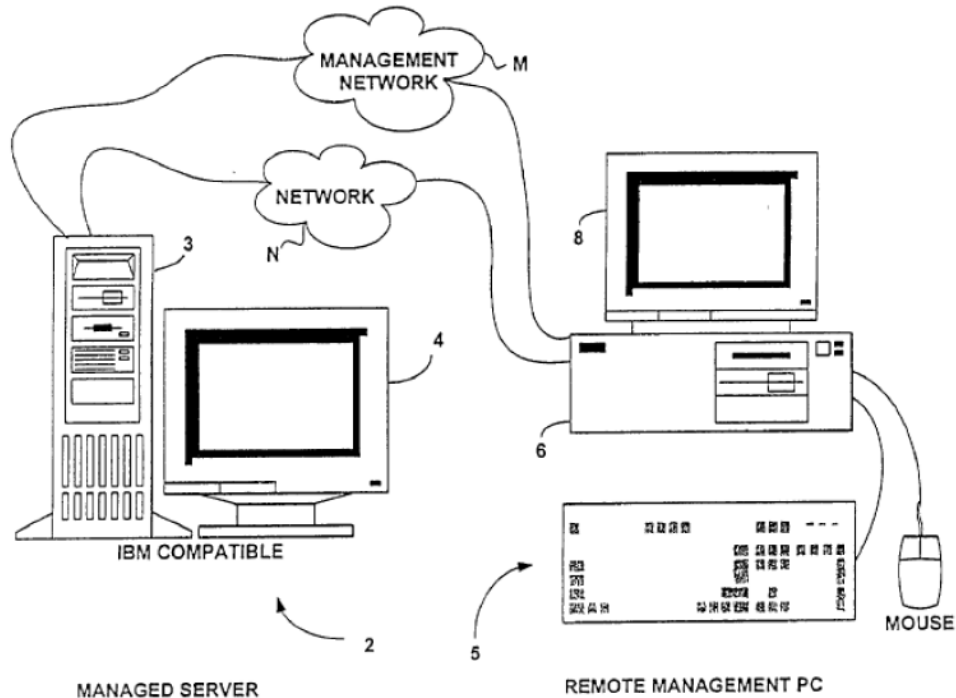


FIG. 1

Figure 1 “is a connection diagram of a managed server and a remote management console according to” Neufeld’s teachings. Ex. 1005 ¶ 25. Petitioner argues that “[i]n Neufeld, the claimed ‘remote device management communication system’ includes one or more managed servers 2 [(i.e., the claimed ‘managed network devices’)] connected to a remote console 5 by a network N and a management network M.” Pet. 21 (citing Ex. 1005 ¶ 34, Fig. 1). According to Petitioner, Neufeld teaches that “[t]he network N can be any sort of network capable of transmitting data between two devices.” *Id.* (citing Ex. 1005 ¶ 35). As illustrated, Neufeld’s managed server 2 includes a CPU 3, Petitioner argues. *Id.* (citing Ex. 1005 ¶ 34, Fig. 1).

Petitioner annotates Neufeld’s Figure 2, as shown below, in support of its arguments. *Id.* at 23.

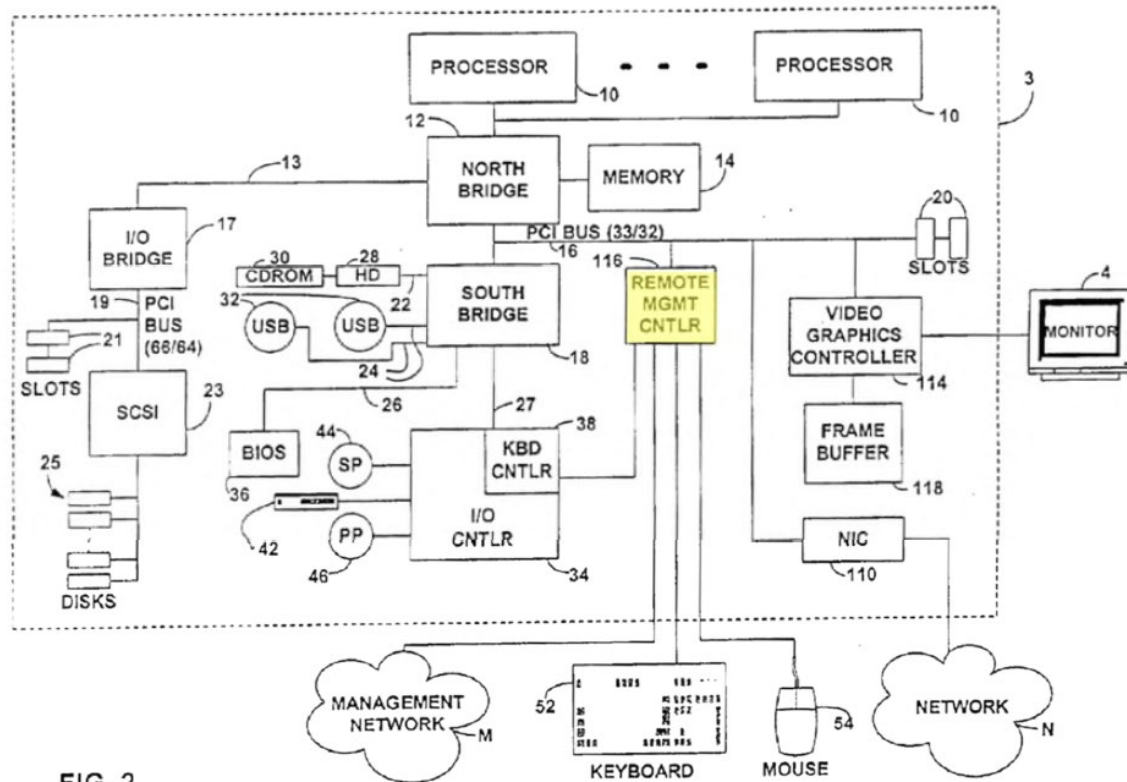


FIG. 2

Figure 2 is a block diagram of a managed server for connection to a remote management console according to Neufeld’s teachings. Ex. 1005 ¶¶ 25–26. Petitioner annotates this figure by coloring in yellow a remote manager controller 116. Pet. 17; Ex. 1005 ¶¶ 43, 45. Petitioner argues that CPU 3 houses the remote server management controller 116, which is the claimed “secure management access controller.” *Id.* at 21. Petitioner adds that Neufeld teaches that the remote server management controller 116 can be implemented as a single application specific integrated circuit (“ASIC”). Pet. 21–22 (citing Ex. 1005 ¶¶ 50–51).

Petitioner annotates Neufeld’s Figure 3, as shown below, in support of its arguments. *Id.* at 23.



Figure 3 “is a block diagram of [a] remote management controller,” in accordance with Neufeld’s teachings. Ex. 1005 ¶ 27. Petitioner annotates this figure by coloring in yellow (i) the remote management controller’s reference numeral “116,” (ii) label “Embedded I/O Controller” and its reference numeral “150,” and (iii) an Input/Output processor (“IOP”) 156. Pet. 23.

Petitioner argues that Neufeld’s embedded I/O controller 150 “includes an Input/Output processor (‘IOP’) 156,” which “is coupled to functional modules of the remote server management controller 116,” and “provides general control and functions as a management processor for the remote server management controller 116.” *Id.* (citing Ex. 1005 ¶ 34, Fig. 3; quoting *id.* ¶ 54). According to Petitioner, Neufeld teaches that the embedded I/O controller 150 also can be implemented as a single ASIC. *Id.* at 21–22 (citing Ex. 1005 ¶ 51).

In addition, Petitioner argues that “[t]he claimed ‘management applications’ are access control and monitoring applications which are performed by the remote server management controller 116 to provide for ‘lights out’ management.” *Id.* at 23 (citing Ex. 1005 ¶ 76). Petitioner argues that “[t]hese applications on the remote server management controller 116 implement critical functions (e.g., booting and powering down the managed server, modifying flash ROM/firmware), moderately critical functions (e.g., altering user profiles, performing or suppressing backups) and non-critical functions (e.g., file/device sharing, altering directories).” *Id.* at 23–24 (citing Ex. 1005 ¶ 80 & Table 1). Moreover, “the IOP 156 dictates control and monitoring functions in managed server 2,” and “securely controls access to management applications by providing to the network device ‘functionality for accessing, interacting, and monitoring the managed server 2,’” according to Petitioner. *Id.* at 24 (quoting Ex. 1005 ¶ 34).

In addition, Petitioner argues that “Neufeld’s remote device management communication system controls communications to and from management applications by establishing an ‘out-of-band communication session with the remote server management controller 116.’” *Id.* (quoting Ex. 1005 ¶ 59); Ex. 1005 ¶ 12 (“Out-of-band communication . . . is not performed across the managed server’s normal connection to the network,” but instead “a ‘back door’ communication channel is established by a remote server management tool . . . using some other interface with the server (such as . . . an Ethernet interface or the Internet).”).

In addition, Petitioner argues that “[t]he claimed ‘distributed network’ includes the devices in networks N and M including the client computers such as managed server(s) 2 and remote management PC(s) 5 as well as other client computers.” Pet. 25 (citing Ex. 1005 ¶¶ 8, 83). “Neufeld further

discloses that the network N can include the public Internet, which inherently includes large numbers of servers, client computers, and devices such as routers,” according to Petitioner. *Id.* (citing Ex. 1005 ¶¶ 35, 88; Ex. 1046 ¶ 96).

In addition, Petitioner argues that the claimed “network services” include sharing of files and printers, Emergency Management services, directory service, and authentication and encryption services. *Id.* (citing Ex. 1005 ¶¶ 7, 74, 76). Petitioner adds that “Neufeld discloses that the network N can include the public Internet, which inherently includes network services such as Domain Name Service.” *Id.* (citing Ex. 1005 ¶¶ 35, 88; Ex. 1046 ¶ 97).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find Petitioner sufficiently shows that Neufeld teaches claim 1’s preamble. In light of our finding, we need not, and thus do not, reach whether claim 1’s preamble is limiting.

2. Secure Management Access Controller

Petitioner argues that Neufeld teaches “at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data,” as recited in claim 1. Pet. 25–28. More specifically, Petitioner argues that Neufeld’s remote server management controller 116 is the claimed “secure management access controller,” and the managed server 2 is the claimed “managed network device.” *Id.* at 21–22, 25–26; *see supra* Section V.B.1 (finding that Neufeld teaches these elements). Petitioner argues that “Neufeld discloses that the remote server management controller 116 is connected to PCI bus 16/172 that is a data bus of the managed server 2.” Pet. 26 (citing Ex. 1005 ¶¶ 43, 57, Figs. 2–3; Ex. 1046 ¶ 99).

In addition, Petitioner argues that “Neufeld further discloses that device management data is communicated to the remote server management controller 116 via the PCI bus 16/172.” *Id.* at 27. In particular, Petitioner argues that “Neufeld discloses that NIC 110 is connected to PCI bus 16/172 as well as the network N . . . , and that the ‘remote management controller 116 connects to . . . the network N . . . to provide functionality for accessing interacting, and monitoring the managed server 2 from the remote console 5.’” *Id.* (quoting Ex. 1005 ¶ 43; citing *id.* ¶¶ 14–15, 22, 44–45) (second and third alterations in original). “Because Neufeld discloses (a) that a management request may be received in-band via Network N/NIC 110, and (b) that NIC[]110 is attached to the same PCI bus 16/172 as the remote server management controller 116, Neufeld discloses that management messages are communicated to the remote server management controller 116 via the connection to the PCI bus 16/172,” according to Petitioner. *Id.* at 27–28 (citing Ex. 1046 ¶ 100).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find Petitioner sufficiently shows that Neufeld teaches this limitation.

3. *Out-of-band Access Connection Means*

Petitioner argues that Neufeld teaches “an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device,” as recited in claim 1. Pet. 28–32. As we conclude above, “an out of band access connection means” is a means-plus-function term (i) with the recited function being “connecting said one or more network services or remote users with said secure management access controller for management of said network device,” and (ii) the

corresponding structures for performing this function including “an Ethernet network” that uses SNMP. *See supra* Section III.

Petitioner argues that “Neufeld’s remote server management controller 116, includes an Ethernet interface 180 connected to a Management Network M to provide the main external communication interface between the remote server management controller 116 and the outside world.” Pet. 28–29 (citing Ex. 1005 ¶ 61, Fig. 3). According to Petitioner, “Neufeld’s Management Network M . . . connect[s] a remote user (e.g., a remote administrator) at remote management PC 5 via network M with the remote server management controller 116 to engage in out-of-band communication of management data with the remote server management controller 116.” *Id.* at 29 (citing Ex. 1005 ¶¶ 43, 62; Ex. 1046 ¶ 104).

In addition, Petitioner argues that it would have been obvious to one of ordinary skill in the art to use SNMP for the out-of-band connection on the Management Network M accessed via the Ethernet interface 180 because, as admitted in the ’140 patent, this protocol is “typically utilized for management of a device.” *Id.* at 31 (quoting Ex. 1002, 12:23–29). Petitioner adds that “employ[ing] SNMP . . . as described in RFC1157 over the Ethernet connection to management network M as the SNMP protocol was very well-known in the art for remotely managing devices.” *Id.* at 31–32 (citing Ex. 1018,¹² 2; Ex. 1046 ¶ 107).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find Petitioner sufficiently shows that Neufeld teaches this limitation.

¹² RFC1157: A Simple Management Network Management Protocol (SNMP) (May 1990).

4. *Virtual Management Interface Connection Means*

Claim 1 further recites “at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller, wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” Ex. 1002, 22:48–51. At this stage, we agree with Petitioner and find Petitioner sufficiently shows that Neufeld teaches this limitation. Pet. 32–34.

As we conclude above, “virtual management interface connection means” is a means-plus-function term with the following recited functions: (i) “connecting said one or more network services or remote users with said secure management access controller”; (ii) “provides logical separation of management data from user data,” and (iii) “utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” *See supra* Section III. And the functions’ corresponding structure is a VPN. *Id.*

We agree with Petitioner and find Petitioner sufficiently shows that Neufeld teaches employing a VPN. *See* Ex. 1005 ¶¶ 9, 22, 88 (Table 4). For example, Neufeld explains the following:

[T]he arrangements of servers and clients in a larger network environment could be connected in any of a large number of topologies that may include local area networks (“LANs”), wide area networks (“WANs”), and municipal area networks (“MANs”). Clients may also have the ability to access these networks via a virtual private network (“VPN”) or via the Internet.

Id. ¶ 9. Furthermore, Neufeld teaches that “if [a] system administrator attempts to access [a] server from a remote terminal located outside of work, such as at home or while traveling,” “the system administrator must typically use the Internet or *a virtual private network* to access the system.” *Id.* ¶ 22 (emphasis added). At this stage, we find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art “would have understood such access involves communications with Neufeld’s remote server management controller 116 given that it is a network administrator that is accessing the server.” Ex. 1046 ¶ 110. This testimony is consistent with Neufeld’s teachings involving remote management. *See* Ex. 1005 ¶¶ 34–35, 59, Figs. 1–3. Thus, we preliminarily find that Neufeld teaches that the VPN performs the function of connecting a remote user (i.e., network administrator) with the secure management access controller (i.e., the remote server management controller 116).

In addition, we agree with Petitioner and preliminarily find that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN for the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N) to provide a dedicated VPN for communications of management data between the managed server 2 and the remote management PC 5. *See supra* Section V.B.2 (finding that Neufeld teaches that network N connects to the NIC 110, which connects to the PCI bus 16/172, which connects to the remote management controller 116 for accessing, interacting, and monitoring the managed server 2 from the remote console 5). Thus, at this stage, we agree with Petitioner and find Petitioner sufficiently shows that Neufeld’s VPN performs the function of using managed server 2’s NIC 110 user interface for in-band communication of management requests which connects the remote user (i.e., network

administrator) with the secure management access controller (i.e., the remote management controller 116).

In addition, at this stage, we agree with Petitioner and find that Neufeld’s teaching of employing the VPN for the above discussed in-band communication of management requests teaches that the VPN performs the function of providing logical separation of management data from user data. Pet. 34. More specifically, we agree with Petitioner and find that Neufeld’s VPN, like the VPN technology of the ’140 patent, provides for the claimed logical separation because the use of the VPN differentiates traffic of the dedicated VPN (i.e., management traffic) from other user traffic (i.e., “user data”). *Id.*; Ex. 1046 ¶¶ 113–114. This understanding is consistent with the Specification of the ’140 patent. *See, e.g.*, Ex. 1002, 6:31–33 (“The VPN technology provides the logical separation, confidentiality, and integrity of the management traffic while it is in transit.”), 7:1–3 (“The VPN tunnels provide for logical separation of the management traffic from any other traffic utilizing the network.”).

Accordingly, based on the record before us, we find unavailing Patent Owner’s arguments that Neufeld does not teach that the VPN “provides logical separation of management data from user data.” Prelim. Resp. 28; *see also id.* at 29, 32–33 (making same argument). As we discuss above, Neufeld’s VPN provides for the claimed logical separation because the use of the VPN differentiates its traffic (i.e., management traffic) from other user traffic (i.e., “user data”), which is not sent over the VPN. We also find unavailing Patent Owner’s arguments concerning inherency for the same reasons discussed above. Prelim. Resp. 23, 29–30, 35.

We also find unavailing Patent Owner’s argument that “Neufeld is actually about user authentication to a network and not the separation of

data.” *Id.* at 24. According to Patent Owner, when Neufeld mentions a VPN, it “is merely used to connect to the network.” *Id.* at 24–27 (citing Ex. 1005 ¶¶ 9, 22, 88, Table 4). First, we disagree that Neufeld is only about user authentication to a network. Rather, Neufeld discusses authentication, encryption, and privileges as separate concepts. *See* Ex. 1005 ¶ 85. For example, Neufeld teaches that “any type of remote access would typically utilize encryption techniques, while direct access may not.” *Id.* And one of ordinary skill in the art would have understood employing a VPN to provide for encryption. *See* Ex. 1046 ¶¶ 111–112. Regardless, we do not limit Neufeld’s teaching of the site administrator using a VPN to remotely connect to the managed server to a specific purpose. *See In re Mouttet*, 686 F.3d 1322, 1331 (Fed. Cir. 2012) (“A reference may be read for all that it teaches, including uses beyond its primary purpose.”).

Second, Neufeld explicitly teaches that a system administrator remotely accessing a server outside of work must typically use a VPN to access the system. Ex. 1005 ¶ 22. At this stage, we find no principled basis for Patent Owner’s argument that one of ordinary skill in the art would have understood Neufeld’s teachings to mean using a VPN only for logging into the network. Prelim. Resp. 27. Would the administrator then use a different unsecure connection (the Internet) to send management messages? In addition, we find this argument is contrary to Neufeld’s teachings we discuss above. Ex. 1005 ¶¶ 9, 22, 85, 88 (Table 4) (showing encryption with the VPN connection).

We also find unavailing Patent Owner’s characterization of Petitioner’s argument regarding the VPN operating “via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N).” Prelim. Resp. 40 (citing Pet. 33). Patent Owner argues that

“such a VPN would merely establish a connection between the system administrator . . . and the NIC 110—not with the remote server management controller 116.” *Id.* Rather, Petitioner argues for “utiliz[ing] a point-to-point VPN with tunneling functionality *on Neufeld’s managed server 2* via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N) in order to provide for a dedicated VPN for communications of management data with the remote management PC 5.” Pet. 33 (emphasis added). Thus, Petitioner does not identify the managed server’s end point as the NIC 110, as Patent Owner suggests, but rather identifies the remote server management controller 116 as it is the management processor for the managed server 2. *See* Pet. 33; *supra* Section V.B.2.

Lastly, we note that Petitioner also argues that a specific VPN implementation would have been obvious. Pet. 32–33. More specifically, Petitioner argues that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN as a point-to-point VPN with tunneling functionality. *Id.* (citing Ex. 1046 ¶ 111). Petitioner argues that such VPN technology is the same as the VPN technology disclosed by the ’140 patent. *Id.* (citing Ex. 1046 ¶ 112).

But this specific implementation is inapposite. The adopted claim construction for this term—which was proposed by Petitioner, not addressed by Patent Owner, and is the construction reached by the district court—identifies a VPN as the corresponding structure, and not a specific VPN implementation. *See supra* Section III; Ex. 1042, 3–4. The parties should consider whether the current construction for “virtual management interface connection means” needs clarification through further claim construction during the trial portion of this proceeding, in accordance with our Rules.

To provide guidance, however, we address below the parties' arguments regarding this VPN implementation. At this stage, we agree with Petitioner and find that one of ordinary skill in the art would have found it obvious to implement Neufeld's VPN as a point-to-point VPN with tunneling functionality. Pet. 33. In particular, at this stage, we find persuasive Dr. Meldal's testimony that one of ordinary skill in the art would have found it obvious, as disclosed in the '140 patent, to implement Neufeld's VPN as a point-to-point VPN with tunneling because such VPN technology was a well-known method for implementing a point-to-point VPN. Ex. 1046 ¶¶ 111–112. We appropriately consider such evidence of the knowledge that one of ordinary skill in the art would have had as part of our obviousness analysis. *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013); *see also KSR*, 550 U.S. at 417 (“When there is a design need or market pressure to solve a problem [(i.e., choosing a VPN)] and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.”).

At this stage, we do not find Dr. Meldal's testimony that VPN tunneling was well-known is conclusory, as Patent Owner argues. Prelim. Resp. 37. We note that Dr. Meldal also testifies that this known point-to-point VPN tunneling also was disclosed by the '140 patent. *See* Ex. 1046 ¶¶ 49 (citing Ex. 1002, 6:24–33), 112; Pet. 3. And the '140 patent seems to admit that VPN tunneling was known. *See* Ex. 1002, 6:26–28 (“The VMI utilizes existing and developing technology such as VPN to build secure tunnels between the SMACC chipset and the management center . . .”). Also, we note that Dr. Goldberg's testimony regarding VPN

using tunneling also seems to support that such was known. *See* Ex. 2001 ¶ 67 (citing Ex. 2004,¹³ 8). The parties should consider, however, addressing this issue further during trial, in accordance with our Rules.

We also find unavailing Patent Owner’s arguments that Petitioner fails to explain why one of ordinary skill in the art would have modified Neufeld. Prelim. Resp. 31, 33–34, 37. Rather, as we discuss above, Petitioner argues, and we agree at this stage, that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN as a point-to-point VPN with tunneling functionality, a known VPN implementation.

In sum, we find Petitioner sufficiently shows that Neufeld teaches this limitation.

5. *Summary*

In summary, at this stage, we determine that Petitioner shows a reasonable likelihood that it would prevail in showing that claim 1 would have been obvious to one of ordinary skill in the art in view of Neufeld.

VI. ANALYSIS OF OTHER CLAIMS AND GROUNDS

Because Petitioner demonstrates a reasonable likelihood of success in proving that at least one claim of the ’140 patent is unpatentable, we institute on all grounds and all claims raised in the Petition. *See* 37 C.F.R.

§ 42.108(a). Therefore, at this stage, it is not necessary for us to provide an assessment of every challenge raised by Petitioner. Those challenges, in our view, are best left for trial after full development of the record.

However, in order to provide guidance to the parties, we address the remaining challenges that are disputed by Patent Owner. *See* CTPG 6 (“If a trial is instituted, the Board generally will provide analysis of the strengths

¹³ Charlie Scott et al., *Virtual Private Networks*, (2d ed. 1999) (Ex. 2004).

and weaknesses of all challenges in the petition in order to provide guidance to the parties for the upcoming trial.”).

A. Summary of IPMI

IPMI “presents the base specifications for the *Intelligent Platform Management Interface* (IPMI) architecture.” Ex. 1020, 23. “The term ‘platform management’ is used to refer to the monitoring and control functions that are built in to the platform hardware and primarily used for the purpose of monitoring the health of the system hardware.” *Id.* “The IPMI specifications define standardized, abstracted interfaces to the platform management subsystem,” “includ[ing] the definition of interfaces for extending platform management between board within the main chassis, and between multiple chassis.” *Id.* In particular, IPMI “defines the overall architecture, common commands, event formats, data records, and capabilities used across IPMI-based systems and peripheral chassis.” *Id.* “This includes the specifications for IPMI management via LAN, serial/modem, PCI Management bus, and the local interface to the platform management.” *Id.*

B. Summary Of Lawrence

Lawrence “relates generally to communication networks[, and m]ore particularly, . . . to a method and system to provide secure in-band management for a packet data network.” Ex. 1043, 1:7–10. More specifically, Lawrence teaches that a “network device is managed using the management traffic received over [a] VPN.” *Id.* at code (57). Lawrence teaches that “[a]n in-band management system is created by configuring a [VPN] for a network device and linking the VPN to a management device or a management function.” *Id.* “By using the VPN to carry management

traffic and to create the in-band management system, management of the network device can be made secure.” *Id.*

C. Disputed Issues

At this stage, the parties dispute whether the combination of IPMI and Lawrence renders claim 1 obvious. In particular, the parties dispute whether (i) Lawrence’s VPN provides logical separation of management data from user data, (ii) IPMI’s LAN controller can be combined with Lawrence’s VPN module, and (iii) one of ordinary skill in the art would have been motivated to combine IPMI and Lawrence. We address these disputes below.

First, at this stage, we find unavailing Patent Owner’s argument that a VPN does not provide logical separation of management data from user data for the same reasons as we discuss above. *See* Prelim. Resp. 46–48; *supra* Section V.B.4.

Second, we find unavailing Patent Owner’s arguments that “[t]he LAN controller in IPMI works by reading the addresses of received packets and routing them to the appropriate entity (in this case, the BMC),” and that “[a]dding a VPN into the mix, allegedly to separate management data from user data, would completely change the operation of the LAN controller from routing data within a network to separating management data from user data.” Prelim. Resp. 51; *see also id.* at 52 (citing Ex 2001 ¶ 80) (arguing that integrating Lawrence’s VPN modules into the LAN Controller would render it inoperable). At this stage, we do not find that these functions are incompatible, but rather the combination Petitioner proposes would allow for both. *See* Pet. 54; Ex. 1046 ¶¶ 158–160; *see also KSR*, 550 U.S. at 420–21 (one of ordinary skill in the art is “a person of ordinary creativity, not an automaton”).

Third, at this stage, we agree with Patent Owner that Petitioner does not show that one of ordinary skill in the art would have had a rational reason to combine IPMI and Lawrence’s teachings as Petitioner does. Prelim. Resp. 51–52. In particular, Petitioner argues that “IPMI does not detail or limit how to implement the side-band interface for . . . in-band communication, and therefore [one of ordinary skill in the art] would have looked to other sources for information as to how to implement IPMI’s side-band interface.” Pet. 52 (citing Ex. 1046 ¶ 156). And Petitioner argues that Lawrence teaches advantages of using the internal secure links to communicate in-band management information. *Id.* at 53 (Ex. 1043, 2:20–58). Petitioner then argues that one of ordinary skill in the art “would have recognized Lawrence’s Internal Management VPN Link 711 in Figure 7 as a desirable and convenient way in which to implement IPMI’s side-band interface, and thus would have found it obvious to include Lawrence’s VPN tunneling technology in IPMI’s Network (LAN) controller in order to implement IPMI’s side-band interface (corresponding to Lawrence’s Internal Management VPN link 711).” *Id.* at 54 (citing Ex. 1046 ¶ 160).

We view Petitioner’s arguments as focusing on IPMI’s side-band interface, and do not address having a VPN connect to the remote user. *See* Pet. 51–54, 64–65. Thus, at this stage, we agree with Patent Owner that Petitioner does not sufficiently show why one of ordinary skill in the art would have been motivated to use a VPN on an internal connection (side-band interface) within a server, absent such security on the external connection portion. *See* Prelim. Resp. 51–52. Similarly, we also find that Petitioner does not clearly explain how the corresponding structure (the VPN) “connect[s] said one or more . . . remote users with said secure management access controller.” *See* Pet. 65.

VII. CONCLUSION

For the foregoing reasons, we determine that Petitioner has shown a reasonable likelihood that it would prevail in proving the unpatentability of at least one of the challenged claims of the '140 patent. We thus institute an *inter partes* review of all of the challenged claims of the '140 patent on all grounds asserted in the Petition.

Any findings or conclusions in this Decision are made only for the purposes of institution and are not dispositive of any issue. We have not made a final determination with respect to the patentability of any challenged claim. Our final determination will be based on the record as fully developed during trial, including any evidence or argument timely presented by the parties under our Rules.

VIII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the '140 patent is instituted on all of the challenged claims and all grounds asserted in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial commences on the entry date of this Decision.

IPR2024-00124
Patent 7,325,140 B2

For PETITIONER:

James M. Heintz
Gianni Minutoli
DLA PIPER LLP
jim.heintz@us.dlapiper.com
gianni.minutoli@us.dlapiper.com

For PATENT OWNER:

Brandon R. Theiss
Daniel H. Golub
Ryan W. O'Donnell
Robert D. Leonard
VOLPE KOENIG
BTheiss@vklaw.com
DGolub@vklaw.com
RODonnell@vklaw.com
RLeonard@vklaw.com

Russell J. Rigby
INTELLECTUAL VENTURES II LLC
rrigby@intven.com